7А

УДК 681.518.9; 621.384.3

С.С. Анцыферов, К.Е. Русанов, Л.В. Маслова
МГТУ МИРЭА, г. Москва
Россия, 119454, г. Москва, пр. Вернадского, 78

Защита информации интеллектуальных систем

S.S. Antsyferov, K.E. Rusanov, L.V. Maslova
Moscow state technical university MIREA, c. Moscow
Russia, 119454, c. Moscow, Vernadsky ave., 78

Information Protection of the Intellectual Systems

С.С. Анциферов, К.Є. Русанов, Л.В. Маслова
МДТУ МІРЕА, м. Москва
Росія, 119454, м. Москва, пр. Вернадського, 78

Захист інформації інтелектуальних систем

Проблема обеспечения защиты информации интеллектуальных систем обработки является одной из важнейших при построении надежной информационной структуры. Эта проблема охватывает физическую защиту данных и системных программ и защиту от несанкционированного доступа к данным, передаваемым по линиям связи и находящимся на накопителях. Несанкционированный доступ может быть результатом деятельности как посторонних лиц, так и специальных программ-вирусов. Не менее важной задачей является оценка качества защиты информации. В данной статье предложена система оценки качества защиты информации интеллектуальных систем с учетом динамики изменения их параметров.

Ключевые слова: интеллектуальная система, система защиты информации, система оценки качества, экспертная система.

The problem of ensuring protection of information of the intellectual systems of processing is one of the major at creation of reliable information structure. This problem covers both physical protection of data and system programs, and protection against unauthorized access to the data transferred on communication lines and being on stores. Unauthorized access is a result of activity of outsiders and special viruses. Not less important task is the quality rating of protection of information. The system of quality rating of protection of information of the intellectual systems is offered in this article subject to the change dynamics of parameters.

Key words: intellectual system, system of protection of information, system of quality rating, expert system.

Проблема забезпечення захисту інформації інтелектуальних систем обробки є однією з найважливіших при побудові надійної інформаційної структури. Ця проблема охоплює фізичний захист даних і системних програм і захист від несанкціонованого доступу до даних, що передаються по лініях зв'язку і перебувають на накопичувачах. Несанкціонований доступ може бути результатом діяльності як сторонніх осіб, так і спеціальних програм-вірусів. Не менш важливим завданням є оцінка якості захисту інформації. У даній статті запропоновано систему оцінки якості захисту інформації інтелектуальних систем з урахуванням динаміки зміни їх параметрів.

Ключові слова: інтелектуальна система, система захисту інформації, система оцінки якості, експертна система.

Введение

При решении широкого круга задач, связанных с передачей и обработкой интенсивных потоков данных, а также хранением информации всё более широко применяются интеллектуальные системы распределённого характера, в частности, для

решения задач медицинской диагностики. Для исключения возможной потери и искажения данных в результате посторонних воздействий создаются системы защиты информации. Основу построения этих систем составляют программные и аппаратно-программные средства: антивирусные и криптографические, архивации данных, идентификации и аутентификации пользователя, протоколирование и аудит, аппаратные ключи защиты, брандмауэры, шифрующие платы, устройства считывания индивидуальных характеристик человека. Вместе с тем интеллектуальные системы с распределёнными параметрами являются динамично развивающимися. Изменениям может подвергаться как аппаратная, так и программная часть, а также конфигурация интеллектуальных систем. Всё это приводит к необходимости создания систем защиты информации, обладающих свойством адаптивности к изменяющимся условиям. Важным моментом для достижения данной цели является разработка критериев оценки качества систем защиты информации. В качестве критериев оценки качества защиты информации, как правило, используются следующие: экономическая эффективность, трудоёмкость, техническая сложность программных и аппаратных средств, надёжность, устойчивость, вероятность преодоления защиты за определённое время, устойчивость к электромагнитному воздействию (возможность считывания информации), вероятность аппаратного сбоя на основании внешних воздействий, вероятность утечки и искажения информации из-за несанкционированных программных воздействий, вероятность снижения уровня защиты при переконфигурировании интеллектуальной системы. Трудности оценки качества защиты обусловлены неопределенностью условий функционирования, а известные методики и рекомендации не учитывают динамику изменения параметров интеллектуальных систем. В данной работе все указанные критерии рассматриваются с точки зрения динамики изменения параметров интеллектуальных систем. Перспективным для решения указанной задачи представляется использование принципов экспертного оценивания критериев оценки качества защиты информации.

Целью данной работы является разработка принципов экспертного оценивания уровня качества защиты информации в интеллектуальных системах обработки с учетом динамики изменения их параметров.

Постановка задачи

При создании нескольких взаимосвязанных центров обработки не всегда есть возможность использовать одинаковые операционные системы (ОС) на всех узлах. При работе с каждой операционной системой могут быть свои особенности: устойчивость операционной системы к вирусам, наличие квалифицированного персонала, специализированное программное обеспечение, совместимое с операционной системой, широта применения операционной системы, управление всеми ресурсами системы, наличие встроенных механизмов, которые прямо или косвенно влияют на безопасность программ и данных, работающих в среде ОС, обеспечение интерфейса пользователя с ресурсами системы, размеры и сложность ОС.

Большинство ОС обладают дефектами с точки зрения обеспечения безопасности данных в системе, что связано с обеспечением максимальной доступности системы для пользователя. Рассмотрим типовые функциональные дефекты ОС, которые могут привести к созданию каналов утечки данных. Каждому ресурсу в системе должно быть присвоено уникальное имя – идентификатор. Во многих системах пользователи не имеют возможности удостовериться в том, что используемые ими ресурсы действительно принадлежат системе. Большинство пользователей выбирают простейшие пароли, которые легко подобрать или угадать. Хранение списка паролей в незашиф-

рованном виде дает возможность его компрометации с последующим несанкционированным доступом к данным. Для предотвращения попыток несанкционированного входа в систему с помощью подбора пароля необходимо ограничить число таких попыток, что в некоторых ОС не предусмотрено. Во многих случаях программы ОС считают, что другие программы работают правильно. При использовании общей памяти не всегда после выполнения программ очищаются участки оперативной памяти (ОП). В случае разрыва связи ОС должна немедленно закончить сеанс работы с пользователем или повторно установить подлинность субъекта. При передаче параметров по ссылке возможно сохранение параметров в ОП после проверки их корректности, нарушитель может изменить эти данные до их использования. Система может содержать много элементов (например, программ), имеющих различные привилегии.

При оценке качества защиты следует учитывать следующие показатели:

– производительность;
– простота обслуживания;
– работа под управлением различных операционных систем;
– тиражирование;
– возможность динамического резервного копирования данных;
– сопряжение различных баз данных друг с другом;
– одновременный доступ нескольких пользователей;
– распределенная обработка транзакций;
– параллельное резервное копирование;
– возможность запрета пользователю непосредственного доступа к данным.

Все эти показатели носят динамический характер. И для обобщенной оценки необходима система количественных критериев, назначаемых экспертами. Учитывая большое количество этих оценок и их динамичность, возникает необходимость в создании соответствующей экспертной системы. В качестве количественных критериев предлагается использовать следующие:

а) относительно баз знаний и данных:
– степень надежности базы данных;
– применимость;
– сложность освоения;
– стоимость;
– производительность;
– требовательность к системным ресурсам;

б) относительно операционных систем:
– стоимость;
– распространенность;
– устойчивость к антивирусным атакам;

в) относительно антивирусных средств:
– требовательность к системным ресурсам;
– обнаружение большинства вирусов;
– успешное «лечение» большинства вирусов;
– оставляет ли «следы» после удаления;
– обнаружение потенциально опасных объектов, которые, возможно, являются новыми вирусами;
– имеют ли место ложные срабатывания при попытке обнаружения потенциально опасных объектов;

г) относительно степени надежности аппаратных средств;

д) применение специализированных программных и аппаратно-программных средств:

– скрытая операционная система;

– аппаратные ключи;

– программные и аппаратно-программные межсетевые экраны;

– средства резервного копирования данных;

е) влияние человеческого фактора:

– уровень квалификации персонала;

добросовестность персонала.

Экспертное оценивание качества защиты

Будем считать, что функционирование системы оценки качества (СОК), связанное с оценкой показателей качества, носит стохастический (вероятностный) характер. Положим в основу алгоритмов функционирования байесовский принцип определения апостериорных распределений векторов показателей качества. Используемое в данных алгоритмах сравнение вычисленных значений апостериорных вероятностей с порогами значимости позволяет, казалось бы, достаточно просто реализовать идею распознавания образов векторов показателей качества. Однако байесовский принцип предполагает наличие существенной априорной информации, носителями которой являются специалисты. В силу этого, получаемые апостериорные вероятностные распределения носят по существу субъективный характер. В связи с этим возникает необходимость в экспертной оценке получаемых результатов. Эта необходимость обуславливается неполнотой, неточностью, а иногда и противоречивостью имеющейся априорной информации и использованием вследствие этого правил правдоподобных рассуждений, не гарантирующих логической истинности того или иного заключения.

Использование экспертных оценок правдоподобия позволит: формализовать правдоподобный вывод; интерпретировать весь ход рассуждений и упорядочить возможные результаты по степени доверия к ним. Всё это выгодно отличает экспертные системы от систем распознавания образов.

В предлагаемой экспертной системе (ЭС) используется общая схема представления знаний в виде системы продукций. Система продукций задаётся своим алфавитом, когда элементарные события выражаются в виде значений переменных из конечного набора. Событие может содержать несколько элементарных событий, связанных операциями конъюнкции и отрицания. На множестве событий обычно задаётся частично определённая функция, отражающая меру определённости или оценку правдоподобия события. Такая система знаний представляет собой сеть вывода, где вершины соответствуют событиям, а ориентированные рёбра определяют переход от одних событий к другим по определённым правилам. В задачу ЭС входит определение оценок правдоподобия для событий, на которых они (оценки) не заданы. Кроме того, ЭС должна производить пересчёт той или иной оценки при изменении оценок других событий, а также коррекцию правил перехода при поступлении новых знаний.

ЭС содержит следующие блоки: БЗ – база знаний, хранящая множество продукций (в общем случае правил); БД – база данных, хранящая данные (рабочая память); И – интерпретатор, решающий на основе имеющихся в системе знаний, предъявленную ему задачу; ЛП – лингвистический процессор, осуществляющий диалоговое взаимодействие с пользователем (экспертом) на естественном для него языке (естественный язык, профессиональный язык, язык графики и т.п.); ПЗ – приобретение знаний; ОД – объяснение действий системы с ответом на вопросы о том, почему некоторые заключения были сделаны или отвергнуты.

ЭС работает в двух режимах: приобретения знаний и решения задач. В режиме приобретения знаний в общении с ЭС участвует эксперт (через посредство инженера по знаниям). В этом режиме эксперт наполняет систему знаниями (правилами), которые позволят ей в режиме решения самостоятельно решать задачи из проблемной области. Эксперт вводит в систему продукции, представляемые на естественном языке. Объединение вновь вводимых продукций с базой знаний осуществляется блоком ПЗ. В режиме решения задач в общении с ЭС участвует пользователь, которого интересует результат, способ получения решения. В этом случае данные о задаче после обработки их лингвистическим процессором поступают в рабочую память (БД). ЛП преобразует входные данные с естественного языка пользователя во внутренний язык системы и преобразует сообщения системы с внутреннего языка в естественный язык. Интерпретатор на основе входных данных, продукционных правил и общих сведений о проблемной области формирует решение задачи. Если ответ системы не понятен пользователю, то он может потребовать, чтобы система объяснила, как этот ответ был получен. Блок ОД сообщает о том, как правила используют информацию пользователя; почему использовались (не использовались) данные правила; какие были сделаны выводы. Все объяснения даются на ограниченном естественном языке.

В составе СОК экспертная система оценки качества и выбора управляющих воздействий выполняет роль вспомогательного элемента и предназначена для объективизации (повышения надёжности) оценок правдоподобия, т.е. полученных апостериорных вероятностных распределений.

В рамках предложенной в данной работе стохастической модели функционирования СОК, для продукционного правила $S \Rightarrow s(l)$ (где S – конъюнкция элементарных событий или их отрицание; s – элементарное событие; l – оценка правдоподобия элементарного события, зависящая от оценки элементарных событий из S и правила перехода от S к s) оценку правдоподобия будем задавать парой условных вероятностей $P(s|S)$ и $P(s|\overline{S})$. Априорную вероятность каждого события будем считать равной 0.5, что соответствует полной неопределённости. ЭС начинает работать, когда становятся известными апостериорные вероятности некоторых событий: $P(S|\varsigma) \neq 0.5$ (ς – факторы, обуславливающие то или иное событие). Применение продукции $S \Rightarrow s$ изменяет апостериорную вероятность $P(s|\varsigma)$ следующим образом:

$$P(s|\varsigma) = P(s|\overline{S}) + \frac{P(s) - P(s|\overline{S})}{P(S)} P(S|\varsigma) \text{ для } 0 \le P(S|\varsigma) \le P(S); \quad (1)$$

$$P(s|\varsigma) = \frac{[P(s) - P(s|S)]P(S) + [P(s|S) - P(s)]P(S|\varsigma)}{1 - P(S)} \text{ для } P(S) \le P(S|\varsigma) \le 1. \quad (2)$$

Другими словами, $P(s|\varsigma)$ линейно интерполируется между $P(s)$ и $P(s|\overline{S})$, если апостериорная вероятность $P(S|\varsigma)$ меньше априорной $P(S)$, т.е. появились сомнения в событии S, и $P(s|\varsigma)$ интерполируется между $P(s)$ и $P(s|S)$, если апостериорная вероятность стала больше априорной, т.е. событие подтверждается.

Следует отметить, что для полностью подтверждённых $(P(S|\varsigma) = 1)$ или полностью опровергнутых $(P(S|\varsigma) = 0)$ событий апостериорная вероятность $P(s|\varsigma)$ равна условной вероятности $P(s|S)$ или $P(s|\overline{S})$ соответственно.

Повышение апостериорной вероятности $P(s|\varsigma)$ за счёт применения продукции $S \Rightarrow s$ повышает оценку правдоподобия

$$l(s|\varsigma) = \frac{P(s|\varsigma)}{P(\bar{s}|\varsigma)} = \frac{P(s|\varsigma)}{1 - P(s|\varsigma)}. \quad (3)$$

Если в базе знаний накоплено несколько продукций, дающих различные оценки правдоподобия

$$S_1 \Rightarrow s\ l_1\ (s|\varsigma),$$
$$S_2 \Rightarrow s\ l_2\ (s|\varsigma),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$S_n \Rightarrow s\ l_n\ (s|\varsigma),$$

то необходимо вычислить оценку

$$l\,(s|\varsigma) = h_1 \ldots h_n\, l(s),$$

где

$$h_i = \frac{l_i\ (s|\varsigma)}{l\,(s)}.$$

При этом предполагается независимость $S_1, \ldots, S_n$.

Оценка правдоподобия продукционных правил определяется по формуле Байеса

$$P(s|S) = \frac{P(s)\,P(S|s)}{P(S)}. \quad (4)$$

Это соотношение может быть использовано для обоснованного выбора оценки показателей качества. Однако полученные таким образом оценки правдоподобия обладают определённой неустойчивостью, т.к. небольшие вариации исходных вероятностей, как правило, задаваемых экспертами, могут приводить к изменениям получаемых оценок, что особенно сказывается вблизи их экстремальных значений. Для устранения неустойчивости можно дополнительно использовать операцию интервального оценивания. В этом случае каждое событие S характеризуется нижней границей $P_н(S)$ вероятности $P(S)$ и нижней границей $P_н(\bar{S})$ вероятности $P(\bar{S})$, т.е.

$$P_н(S) \le P(S) \le 1 - P_н(\bar{S}).$$

Если S есть конъюнкция $s_1 ... s_n$, то согласно тождествам теории вероятности, это означает, что имеют место следующие ограничения:

$$\begin{gathered} P_н(S) \ge 1 - \sum_i [1 - P_н(s_i)], \\ P_н(\bar{S}) \ge P_н(\bar{s}_i), \\ P_н(s_i) \ge P_н(S), \\ P_н(\bar{s}_i) \ge P_н(\bar{S}) - \sum_{j \ne i} [1 - P_н(s_j)]. \end{gathered} \quad (5)$$

Изменения значений оценок $P_н(S)$ и $P_н(\bar{S})$ для события $P(S)$ приводят к пересчёту всех вершин сети вывода, в которые ведут пути из S. Пересчёт осуществляется на основе системы неравенств (5) и проводится независимо для $P_н(S)$ и $P_н(\bar{S})$. Противоречием считается ситуация, когда для некоторого s установлено $P_н(S) + P_н(\bar{S}) > 1$. В этом случае включается процедура поиска лучших минимальных изменений в первоначальных оценках, ликвидирующих противоречивость.

Проектирование ЭС существенно отличается от проектирования обычного программного продукта. Использование при их проектировании методологии, принятой в традиционном программировании, либо чрезмерно затягивает процесс создания ЭС, либо вообще приводит к отрицательному результату. Неформализованность указанных задач, отсутствие завершённой теории ЭС и методологии их проектирования приводит к необходимости модифицировать принципы и способы построения ЭС, как в ходе процесса их проектирования, так и создания наукоёмкого продукта, по мере того, как увеличиваются знания разработчиков о проблемной области. В связи с этим целесообразно использование концепции «быстрого прототипа». Согласно этой концепции, вначале создаётся прототип ЭС, который должен удовлетворять двум противоречивым требованиям: решать задачи конкретного приложения; трудоёмкость его разработки должна быть весьма незначительной.

Предлагаемый принцип экспертного оценивания был практически апробирован при решении задачи управления качеством защиты информации интеллектуальной системы обработки диагностической информации, полученной с помощью компьютерной томографии. Преобразование прототипа ЭС в конечный продукт приводит к перепрограммированию ЭС на языках низкого уровня, обеспечивающих как увеличение быстродействия ЭС, так и уменьшение занимаемой ею памяти.

Выводы

В статье рассмотрены основные положения, связанные с оценкой качества защиты интеллектуальных систем. Для решения поставленной задачи предложен принцип экспертного оценивания системы защиты информации в интеллектуальных системах. Предварительные испытания предложенного принципа показали его достаточную эффективность при оценивании уровня качества защиты информации в интеллектуальных системах обработки с учетом динамики изменения их параметров.

Литература

1. Анцыферов С.С. Общие принципы построения и закономерности функционирования интеллектуальных систем / С.С. Анцыферов // Искусственный интеллект. – 2011. – № 3. – С. 6-15.
2. Методология адаптивного управления качеством наукоемкой продукции / [Сигов А.С., Анцыферов Е.С., Голубь Б.И., Анцыферов С.С.] // Искусственный интеллект. Интеллектуальные и многопроцессорные системы: ИИИМС 2006 : материалы МНТК. – Таганрог ; Донецк ; Минск, 2006. – Т.1. – С. 21-25.
3. Системные принципы управления качеством проектирования адаптивных информационно-распознающих систем / [Сигов А.С., Анцыферов Е.С., Голубь Б.И., Анцыферов С.С.] // Известия ТРТУ. – 2005. – № 10. – С. 167-174.
4. Управление качеством синтеза структуры адаптивных информационно-распознающих систем / [Сигов А.С., Анцыферов Е.С., Голубь Б.И., Анцыферов С.С.] // Интеллектуальные и многопроцессорные системы: ИМС 2005 : материалы МНТК. – Таганрог ; Донецк ; Минск, 2005. – Т. 1. – С. 104-109.
5. Адаптивное управление качеством интеллектуальной продукции / [Сигов А.С., Анцыферов Е.С., Голубь Б.И., Ширяев С.В.] // Известия ТРТУ. – 2004. – № 9. – С. 15-20.
6. Экспертное управление качеством интеллектуальной продукции / [Сигов А.С., Анцыферов Е.С., Голубь Б.И., Ширяев С.В.]. // Искусственный интеллект. Интеллектуальные и многопроцессорные системы : материалы МНТК. – Таганрог ; Донецк, 2004. – Т. 2. – С. 63-67.
7. Сигов А.С. Управление качеством проектирования адаптивных информационно-распознающих систем с программируемой структурой / А.С. Сигов, Е.С. Анцыферов, Б.И. Голубь // Фундаментальные проблемы радиоэлектронного приборостроения : материалы МНТК – INTERMATIC-2004. – Москва, 2004. – С. 193-195.
8. Анцыферов С.С. Адаптивные информационно-распознающие системы / С.С. Анцыферов, Н.Н. Евтихиев // Известия ТРТУ. – 2004. – № 9. – С. 183-190.
9. Анцыферов С.С. Метрология виртуальных систем / С.С. Анцыферов // Измерительная техника. – 2003. – № 5. – С. 17-21.

10. Информационная безопасность открытых систем / [Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В.]. – Москва : Горячая линия - Телеком, 2008.
11. Прохода А.Н. Обеспечение Интернет-безопасности / А.Н. Прохода. – Москва : Горячая линия – Телеком, 2008.

Literatura

1. Antsyferov S.S. Iskusstvennyj intellect. 2010. № 3. S. 6-15.
2. Sigov A.S., Antsyferov E.S., Golub B.I., Antsyferov S.S. Materialy MNTK "Iskusstvennyj intellekt. Intellektualinye i mnogoprocessornye sistemy: IIIMS 2006". Taganrog-Donetsk-Minsk. 2006. T. 1, S. 21-25.
3. Sigov A.S., Antsyferov E.S., Golub B.I., Antsyferov S.S. Izvestiya TRTU. 2005. № 10. S. 167-174.
4. Sigov A.S., Antsyferov E.S., Golub B.I., Antsyferov S.S. Materialy MNTK "Intellektualinye i mnogoprocessornye sistemy: IIIMS 2005". Taganrog-Donetsk-Minsk.2005. T. 1, S. 104-109.
5. Sigov A.S., Antsyferov E.S., Golub B.I., Shiryaev S.V. Izvestiya TRTU. 2004. № 9. S. 15-20.
6. Sigov A.S., Antsyferov E.S., Golub B.I., Shiryaev S.V. Materialy MNTK "Iskusstvennyj intellekt. Intellektualinye i mnogoprocessornye sistemy: IIIMS 2004". Taganrog-Donetsk. 2004. T. 2, S. 63-67.
7. Sigov A.S., Antsyferov E.S., Golub B.I. Materialy MNTK "Fundamentalinye problemy radioelektronnogo priborostroeniya - INTERMATIC-2004". Moskva. 2004, S. 193-195.
8. Antsyferov S.S., Evtihiev N.N. Izvestiya TRTU. 2004. № 9. S. 183-190.
9. Antsyferov S.S. Izmeritelinaya tehnika. 2003. № 5. S. 17-21.
10. Zapechnikov S.V., Miloslavskaya N.G., Tolstoy A.I., Ushakov D.V. Informacionnaya bezopasnosti otkrytyh sistem. // Moskva, "Goryachaya liniya - Telekom", 2008.
11. Prohoda A.N. Obespechenie Internet-bezopasnosti. // Moskva, "Goryachaya liniya - Telekom", 2008.

S.S. Antsyferov, K.E. Rusanov, L.V. Maslova

Information Protection of the Intellectual Systems

At the solution of a wide range of the tasks connected with transfer and processing of intensive data flows, and also storage of information more and more widely applies intellectual systems of the distributed character, in particular, to the solution of problems of medical diagnostics. For an exception of possible loss and distortion of data as a result of extraneous influences systems of protection of information are created. A basis of creation of these systems make program and hardware and software: anti-virus and cryptographic, archivings of data, identifications and authentifications of the user, recording and audit, hardware locks of protection, the fireproof walls ciphering payments, devices of reading of individual characteristics of the person. At the same time intellectual systems with the distributed parameters are dynamically developing. To changes can be exposed both hardware, and a program part, and also a configuration of intellectual systems. All this results in need of creation of systems of protection of information, possessing property of adaptability to changing conditions. An important point for achievement of this purpose is development of criteria of an assessment of quality of systems of protection of information. As criteria of an assessment of quality of protection of information the following is, as a rule, used: economic efficiency, labor input, technical complexity program and hardware, reliability, stability, probability of overcoming of protection in a definite time, stability to electromagnetic influence (possibility of reading of information), probability of hardware failure on the basis of external influences, probability of leak and information distortion because of unauthorized program influences, probability of decrease in level of protection at a reconfiguration of intellectual system. Difficulties of an assessment of quality of protection are caused by uncertainty of operating conditions, and known techniques and recommendations don't consider dynamics of change of parameters of intellectual systems. In this work all specified criteria are considered from the point of view of dynamics of change of parameters of intellectual systems. Perspective for the solution of the specified task use of principles of expert estimation of criteria of an assessment of quality of protection of information is represented.

Статья поступила в редакцию 19.12.2011.